

UNITED STATES DISTRICT COURT

for the
District of New Mexico**FILED**UNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICOIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information associated with the Google, LLC Android
profile associated with IMEI – 355604085647493, and/or
phone number (575)936-9494

Case No. 18MR896 SEP 21 2018

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

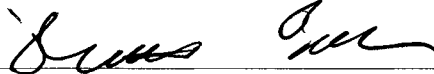
- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1201(a)(1)	Kidnapping
18 U.S.C. § 2119	Carjacking
18 U.S. Code § 1951	Interference with Commerce by Threats or Violence (Hobbs Act)

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Daniel Fondse, Special Agent - FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 09/21/2018

City and state: Albuquerque, New Mexico



Judge's signature

Laura Fashing, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR NEW MEXICO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
GOOGLE, LLC ANDROID PROFILE
ASSOCIATED WITH **IMEI –
355604085647493**, AND/OR **PHONE
NUMBER – (575)936-9494** THAT IS
STORED AT PREMISES OWNED,
MAINTAINED, CONTROLLED, OR
OPERATED BY GOOGLE LLC

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Fondse, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Google, LLC Android profile associated with **IMEI – 355604085647493**, and/or **phone number – (575)936-9494** that is stored at premises owned, maintained, controlled, or operated by Google LLC., a company headquartered in Mountain View, California.. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since May, 2017. Prior to that I was a sworn law enforcement officer in San Diego,

California, for three years. I am currently assigned to the FBI's Albuquerque Division Violent Crime Program, as such, I am authorized to investigate violent crimes, including Kidnapping.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1201(a)(1) - Kidnapping, 18 U.S.C. § 2119 - Carjacking, 18 U.S. Code § 1951 - Interference with Commerce by Threats or Violence (Hobbs Act), 18 U.S.C. § 371 - Conspiracy, and 18 U.S.C. § 2 - Aiding and Abetting have been committed by Megan Bicondova. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

PROBABLE CAUSE

5. On July 26, 2018 a kidnapping was reported to the Federal Bureau of Investigations (FBI), Albuquerque Division. The reporting party stated they were unable to locate or contact the victim, a family member. The reporting party stated they received approximately five phone calls on July 26, 2018 from person(s) alleging to have kidnapped the victim and who demanded money from the reporting party. The phone number used to place the calls to the reporting party was blocked. By analyzing cellular phone records obtained through exigent circumstances, FBI personnel determined phone number 505-582-4555 placed five phone calls on July 26, 2018 to the reporting party, which corresponded to the times the reporting party was contacted by the alleged kidnapper(s). T-Mobile records show the subscriber of 505-582-4555 is Jose Ramirez and the subscriber name effective date was July 03, 2018. The

kidnapping victim later stated Jose Ramirez was known to them. Ramirez is currently the subject of an active federal arrest warrant issued on July 27, 2018 for alleged violation of 18 U.S.C. § 1201(a)(1) - Kidnapping, 18 U.S.C. § 2119 - Carjacking, 18 U.S. Code § 1951 - Interference with Commerce by Threats or Violence (Hobbs Act), 18 U.S.C. § 371 - Conspiracy, and 18 U.S.C. § 2 - Aiding and Abetting in relation to the previously described incidents. Due to the nature of the offenses he may be aware of the law enforcement investigation into this incident and may be taking active measures to avoid law enforcement. Ramirez's location remains unknown.

6. Cell phone records show on July 26, 2018, 575-936-9494 placed at least two calls to 505-582-4555 (Jose Ramirez's phone), during the time the kidnapping victim was held against his will. Furthermore, records showed approximately 50 attempted contacts between the 575-936-9494 and Jose Ramirez's phone in the approximate three days following the kidnapping. . A law enforcement records check through open source databases showed the current user of 575-936-9494 is Megan Bicondova

7. Pre-dawn video from outside the victim's residence on the morning of the kidnapping showed a pick-up truck with what appeared to be light(s) on the roof and a utility rack in the bed drive past the victim's driveway. The vehicle returned several seconds later and stopped near the victim's driveway, before driving out of the neighborhood. The video showed very little vehicle traffic in the victim's neighborhood until the time of the alleged kidnapping, approximately 70 minutes later.

8. On July 27, 2018, the owner of a 1997 Dodge pick-up reported it stolen from the residence at which Jose Ramirez stayed for approximately two weeks, terminating approximately

two days before the kidnapping. The pickup was owned by a family member of Jose Ramirez who regularly left the keys inside the vehicle.

9. On August 10, 2018, the stolen Dodge pick-up was recovered in Albuquerque, NM. The person in possession of the Dodge pick-up, F.M., told your affiant he purchased the vehicle from a female who identified herself as Megan on approximately the day after the kidnapping. F.M. positively identified Megan Bicondova in a photo lineup as the female who sold him the Dodge pick-up. The Dodge pickup had a utility rack and lights on the roof and was visually similar to the vehicle observed on video stopping in front of the victim's residence shortly before the kidnapping.

10. The victim of the kidnapping stated a female was present at a location of his captivity. He described her as 5'6" in height with shoulder-length dirty blond hair, and a stocky, not skinny, build. Megan Bicondova's New Mexico Motor Vehicle Department information shows she was 5'3" in height, weighting 230 lbs, with shoulder-length, brown hair. F.M. described the woman who sold him the Dodge Pick-up as about 5'7" to 5'8" in height, with brown hair just past shoulder length and a very heavy build.

11. On August 14, 2018 Megan Bicondova was interviewed by investigators. She denied any involvement in any kidnapping. Bicondova allowed investigators to look through her cell phone, which she stated was assigned call number 575-936-9494. The cell phone appeared to run on an Android operating system. Her call history before July 27, 2018 had been deleted from the phone. Bicondova said her phone deleted the calls on its own, she didn't delete them.

12. Analysis of cellular phone records obtained from T-Mobile USA indicate the phone number 575-936-9494 was associated with IMEI 355604085647493 from May 26, 2018 to August 22, 2018, with the exception of parts of August 21 and August 22, 2018 when it was

associated with a different IMEI. This included the entire time period for which records were obtained.

13. Your Affiant knows from training, experience and other law enforcement officers that a majority of the population in the United States have cell phones and many cell phones are smart phones. Criminals frequently use electronic devices, such as cellular phones, to coordinate and promote criminal acts. These communications can be in the form of calls, text messages, emails or messages sent on messaging applications and can include content consisting of written text, photos or videos. Information relating to the content of communications as well as preserved location information, including metadata associated with stored files, is often useful and relevant as evidence in criminal investigations.

14. Furthermore, a large majority of smart phones use software operating systems from Apple and Google. They are named iOS (Apple) and Android (Google). As of early 2017, Google's Android operating system had over 87% of the market share of phone operating systems in the United States. There are four cell phone carriers in the country that own a vast majority of working cell phone towers. Those carriers are AT&T, Sprint, T-Mobile and Verizon Wireless. Cell phone carriers keep records of the make, model and unique identifiers of every cell phone that uses their cell towers. One of the most common unique identifiers on a cell phone is the International Mobile Equipment Identifier (IMEI).

15. When a smartphone using the Android operating system is activated, a user is asked to login with a Google owned email address, like example@gmail.com. As part of their normal operation of business, Google stores on their servers the login to the phone and records information about the phone that the user is logging in from. Furthermore, Google, LLC keeps these records and can help identify what Google account used a cell phone by linking the IMEI

with the Google Android registration. The IMEI that Google keeps on other devices on a Google account can be traced back to a cellular phone with the help of the cellular providers. Android cell phones can keep a vast amount of data that relates to use of the phone. Most of this data is stored in databases on the phone, and your Affiant is familiar with the structure and basic operation of databases. On the Android operating system, when Google Mobile Services (GMS) applications, like YouTube, Gmail, Maps are opened, the operating system attempts to log the nearest connected cellular tower or WiFi connection. The phone stores this in a database, which can allow an examination to see when certain applications are opened and approximate locations of the device. Aside from these locations, Google has a service that uploads the location of Android devices to the account that it is registered to. This location history on Google's servers is more accurate as it uses GPS technologies on the device to report back, as opposed to other methods that use cellular towers to approximate locations. Operating systems such as Google's Android or Apple's iOS also assign a resettable, thirty-two (32) character, universally unique, hexadecimal identifier for advertising to cellular devices which operate their applications.

16. Phone carriers also assign users an IMSI (international mobile subscriber identity) that tracks the user across their network. This number can be taken from a phone and given to a wireless phone carrier to identify the account associated with that number.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

17. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized

persons will review that information to locate the items described in Section II of Attachment B. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

18. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

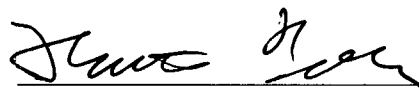
CONCLUSION

19. Based on the forgoing, I request that the Court issue the proposed search warrant.

20. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

21. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.
22. This affidavit was reviewed by Supervisory Assistant United States Attorney Jack Burkhead.
23. The information in this document is true and correct to the best of my knowledge.

Respectfully submitted,



Daniel Fondse
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on September 21, 2018


UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Google, LLC Android profile associated with **IMEI – 355604085647493**, and/or **phone number – (575)936-9494** that is stored at premises owned, maintained, controlled, or operated by Google LLC., a company headquartered in Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC, (“Google”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for any profiles listed in Attachment A from **May 26, 2018 to September 21, 2018**:

- (a) **Location Data:** Any location data currently stored in relation to the phone number identified in Attachment A or associated with the Device ID listed in Attachment A or any other profile or email account associated with these identifiers. This includes any historical physical addresses, latitude and longitude data, estimated latitude and longitude location data, location history, or any other data captured and stored by Google, LLC by the listed user that would aid law enforcement in establishing historical location information related to the Google account use.
- (b) This further includes all information stored and maintained the “My Activity” associated with any profile or Gmail account related to the IMEI or phone number listed in Attachment A. Specifically, all information currently stored in reference to the users “Timeline in Google Maps.”

- (c) Location information can be in the form of historical records. Specific to Google, LLC, this includes any reports of device activity with the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information.
- (d) Any and all unhashed, raw, Advertising Identifiers (Ad IDs) for cellular devices associated with any and all Google accounts linked to the IMEI or phone number listed in Attachment A. These thirty-two (32) character, universally unique, hexadecimal identifiers are formatted in an 8-4-4-4-12 pattern. Both current, and all historical Ad IDs or IDFAs are required to be provided.
- (e) **Account Information:** To include all account owner/user identification information, to include all information listed in the “your personal info” within the Google My Account screen. This includes any stored data that would aid in identifying the user/owner of any accounts or profiles associated with the phone number or IMEI listed in Attachment A. This further includes any IP addresses related data access, logins, or browsing history, forwarding phone numbers, SMS forwarding numbers, alternative email addresses, and any linked social media accounts.
- (f) Further included in “account information” is all information currently stored in reference to the users account to include, Google search history, websites visited history, map search history, and any other information associated with location history, device information and recently used devices.
- (g) **Application History:** To include all apps downloaded from the Google Play Store to the current devices associated with this Gmail address. This request

includes the association of each app to a specific device when available and the date the app was downloaded.

- (h) **Email Content:** Any email content, including sent, received or deleted emails, currently stored in relation to any email address or device associated with the phone number identified in Attachment A or the IMEI identified in Attachment A.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, of violations of 18 U.S.C. § 1201(a)(1) - Kidnapping, 18 U.S.C. § 2119 - Carjacking, 18 U.S. Code § 1951 - Interference with Commerce by Threats or Violence (Hobbs Act), 18 U.S.C. § 371 - Conspiracy, and 18 U.S.C. § 2 - Aiding and Abetting involving Megan Bicondova including information pertaining to the following matters:

- (i) All communications between Megan Bicondova and any other person as they relate to the planning or execution of any of the crimes identified in this document.
- (j) Information identifying the physical locations of Megan Bicondova or any other person as they relate to the crimes identified in this document.
- (k) All photos, metadata or statements constituting evidence of a crime identified in this document.
- (l) Evidence indicating how and when any Google account or profile related to the IMEI or phone number identified in Attachment A was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Google account or profile.
- (m) Evidence indicating the Google profile or account owner's state of mind as it relates to the crimes under investigation;
- (n) The identity of the person(s) who created or used the Google account or profile, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature